UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

Rafael Lora, individually, and on behalf of himself and all others similarly situated, Plaintiff, v. Bartlett Dairy, Inc. Defendant.	Case No. **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiff Rafael Lora ("Plaintiff"), on behalf of himself and all others similarly situated ("Class Members"), files this Class Action Complaint ("Complaint") against Defendant Bartlett Dairy, Inc. ("Defendant") and complains and alleges upon personal knowledge as to themselves and information and belief as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to safeguard and secure the personally identifiable information ("PII") of approximately thousands of individuals, including Plaintiff. The individuals affected are former and current employees of Defendant, whose PII was maintained by Defendant.

2. The data reportedly exposed in the breach includes some of the most sensitive types of data that cybercriminals seek in order to commit fraud and identity theft. As a result of Defendant's negligence, on or prior to June 21, 2023, cybercriminals were able to gain access to Defendant's computer records and access this sensitive and valuable PII (the "Data Breach").[1]

[1] *See* Letter sent by Bartlett Dairy to Plaintiff, Notice of Data Security Incident (Mar. 26, 2024) (attached as Exhibit 1) ("Notice Letter") at 1.

3. According to Defendant, information disclosed in the Data Breach includes, but is not limited to, each affected individual's name, Social Security Number, and Driver License or State ID Number.[2]

4. Bartlett Dairy was founded in 1963 and is "a door-to-door home-delivery and retail milk route in Queens, New York."[3]

5. According to a notice letter sent by Defendant to victims of the data breach (the "Notice Letter"), "[o]n June 21, 2023, [Defendant] identified unusual activity in [its] computer network, which was subsequently confirmed to be the result of a malicious encryption event."[4] Defendant continues to claim:

> We immediately took steps to contain the activity and engaged a cybersecurity firm to investigate what happened and help determine whether any sensitive data was affected. Through that investigation, we learned of information suggesting that an unknown actor gained unauthorized access to our network and acquired certain files, some of which may have contained individuals' personal information. We then worked with additional experts to conduct a comprehensive review of the impacted data to determine what personal information was involved and to identify the individuals who may have been affected. At the conclusion of that review, we worked diligently to collect up-to-date mailing addresses in order to provide notification of this incident to impacted individuals. We completed those efforts on February 27, 2024 and arranged for notification letters to be sent as soon as possible.[5]

[2] *Id.* at 1.

[3] *About Us*, BARTLETT, https://www.bartlettny.com/about-us.php (last visited Apr. 5, 2024).

[4] Notice Letter, *supra* n.1 at 1.

[5] *Id.*

6. Despite learning of the Data Breach over nine months beforehand, Defendant did not begin alerting Plaintiff and other victims of the Data Breach until approximately March 26, 2024.[6]

7. Armed with the PII accessed in the Data Breach, data thieves can commit a variety of crimes, including opening new financial information in Class members' names, taking out loans in Class members' names, using Class members' names to obtain medical services, and using Class members' PII to target other phishing and hacking intrusions.

8. Defendant owed a non-delegable duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII against unauthorized access and disclosure. Defendant breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect its employees' PII from unauthorized access and disclosure.

9. As a result of Defendant's inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiff's and Class members' PII was accessed and disclosed. This action seeks to remedy these failings and the harm caused to Plaintiff and Class members as a result. Plaintiff brings this action on behalf of himself and all persons whose PII was exposed as a result of the Data Breach.

10. As a result of the Data Breach, Plaintiff and Class members have been exposed to a heightened and imminent risk of financial fraud and identity theft. Plaintiff and Class members must now and in the future closely monitor their financial accounts to guard against identity theft.

11. Plaintiff seeks remedies including, but not limited to, compensatory damages, treble damages, punitive damages, reimbursement of out-of-pocket costs, and injunctive relief, including

[6] *See id.*

improvements to Defendant's data security system, future annual audits, and adequate credit monitoring services funded by Defendant.

12. Plaintiff, on behalf of himself and all other Class members, asserts claims for negligence, negligence per se, breach of fiduciary duty, breach of implied contract, and unjust enrichment and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

13. Plaintiff Rafael Lora is a Pennsylvania resident. On or after March 26, 2024, Plaintiff received a letter from Defendant notifying him that his PII was among the information accessed by cybercriminals in the Data Breach.[7]

14. Had Plaintiff known that Defendant would not adequately protect his and Class members' PII, he would not have engaged in employment by Defendant and would not have provided his PII to Defendant or any of its affiliates.

15. Defendant Bartlett Dairy, Inc. is a corporation maintaining its principal place of business at 90-04 161st Street, Jamaica, New York 11432. Defendant is a food distributor with three locations in New York and serves customers in New York, New Jersey, and Pennsylvania.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2) because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendant's citizenship, and (c) the aggregate matter in controversy exceeds $5,000,000, exclusive of interests and costs.

[7] *See id.*

17. This Court has diversity jurisdiction over Plaintiff's claims pursuant to 29 U.S.C. § 1332(a)(1) because Plaintiff and Defendants are citizens of different states and the amount in controversy exceeds $75,000.

18. This Court has general personal jurisdiction over Defendant because Defendant maintains its principal place of business in Jamaica, New York, regularly conducts business in New York, and has sufficient minimum contacts in the State. Defendant engaged in the conduct underlying this action in New York, including the collection, storage, and inadequate safeguarding of Plaintiff's and Class members' PII. Defendant intentionally availed itself of this jurisdiction by entering into employment contracts, marketing and selling products and services, and accepting and processing payments for those products and services within the State.

19. Venue is proper in this District pursuant to 28 U.S.C. § 1391(d). New York has more than one judicial district; Defendant is a corporation currently subject to personal jurisdiction in New York; and if this District was a separate state, Defendant's contacts with this District would subject it to personal jurisdiction in this District because Defendant entered into consumer transactions and provided services and products to customers residing in this District. Therefore, Defendant resides in this District for purposes of venue.

FACTUAL ALLEGATIONS

Overview of Defendant

20. Defendant is a family-owned business that "specializes in custom distribution of frozen foods, dairy and paper products."[8]

[8] *Bartlett Careers*, BARTLETT, https://bartlettny.com/careers.php (last visited Apr. 5, 2024).

21. Defendant was incorporated in 1990, and it now "includes more than 800 perishable and non-perishable items" and maintains "a fleet of more than 100 tractor-trailers and straight trucks[.]"[9]

22. Plaintiff and Class members are or were employees of Defendant.

23. To obtain employment, employees like Plaintiff and Class members are required to provide Defendant directly with sensitive PII.

24. In the regular course of its business, Defendant collects, stores, and maintains the PII it receives from employees who work for Defendant.

25. By creating and maintaining massive repositories of PII, Defendant has provided a particularly lucrative target for data thieves looking to obtain, misuse, or sell such data.

The Data Breach and Notice Letter

26. On June 21, 2023, Defendant identified unusual activity in its computer network, which, at an unspecified subsequent date, Defendant confirmed "to be the result of a malicious encryption event."[10]

27. Defendant states, without further specification, that it "immediately took steps to contain the activity" and retained "a cybersecurity firm to investigate what happened and help determine whether any sensitive data was affected."[11] That first investigation revealed to

[9] *See A Brief History*, BARTLETT, https://bartlettny.com/a-brief-history.php (last visited Apr. 5, 2024).

[10] *See* Notice Letter, *supra* n.1 at 1.

[11] *Id.*

Defendant that "an unknown actor gained unauthorized access to [its] network and acquired certain files, some of which may have contained individuals' personal information."[12]

28. Defendant next engaged "additional experts" to review what PII and which individuals were affected by the Data Breach.[13]

29. At the conclusion of that review, at a date unspecified, Defendant "collected up-to-date mailing addresses" of the impacted individuals so it could provide written notification, and that project was completed on February 27, 2024.[14]

30. Lastly, Defendant "arranged for notification letters to be sent out as soon as possible[,]" and they were mailed on approximately March 26, 2024.[15]

31. The Notice Letter Defendant provided to victims of the Data Breach is glaringly deficient.[16]

32. Defendant waited more than nine months from the date it learned of the Data Breach to directly notify affected individuals.[17]

33. To date, Defendant has not disclosed crucial information, including, but not limited to how many of its employees were affected by the Data Breach; how the cybercriminals were able to exploit vulnerabilities in Defendant's IT security systems; the steps taken by Defendant when it

[12] *Id.*

[13] *Id.*

[14] *Id.*

[15] *Id.*

[16] *See id.*

[17] *See id.*

allegedly took steps to protect its systems and contain the cybercriminal activity; the identity of the hacking group responsible for the Data Breach; the identities of the cybersecurity firms Defendant engaged with to address the Data Breach or the reason(s) why Defendant had to undergo two separate investigations with different cybersecurity firms; when each of the investigations was completed, or any reasoning for why Defendant waited over nine months to provide written notification, or the specific measures, if any, Defendant has since taken to enhance its security safeguards.

34. While Defendant has not disclosed the exact data obtained in the Data Breach, its Notice Letter informed Plaintiff and Class members that the data likely consists of PII including, but not limited to, names, Social Security numbers, and Driver's License or State ID numbers.[18]

35. Defendant recognizes the long-term risks to Plaintiff and Class members resulting from the Data Breach, as evidenced by their recommendation in the Notice to "remain vigilant for incidents of fraud and identity theft by reviewing account statements and credit reports closely."[19]

36. Despite the ongoing and long-term risks of financial fraud and identity theft for victims of the Data Breach, Defendant does not provide sufficient identity protection services for the affected individuals.[20]

37. While Defendant offers complimentary credit monitoring and identity theft protection services, it places the burden on Data Breach victims to sign up for these services within less than two months, and the services are only offered for twelve months, as affected individuals

[18] *See id.*

[19] *See id.* at 2.

[20] *See id.* at 1-2.

are required to enroll in the services by June 26, 2024, exactly two months from the date the Notice Letter was mailed.[21]

38. Cybercriminals hacked Defendant's systems containing Plaintiff's and Class members' PII, which was accessible, unencrypted, unprotected, and vulnerable to acquisition and/or exfiltration by the unauthorized actor.

39. Plaintiff and Class members provided their PII to Defendant, either directly or indirectly, with the reasonable expectation and mutual understanding that Defendant would comply with its obligation to keep such information confidential and secure from unauthorized access.

40. Defendant also benefited directly from the PII provided by Plaintiff and Class members. Defendant collected and utilized Plaintiff's and Class members' PII in the course of employing them, thus using their PII to enhance and grow its business.

41. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class members' PII, Defendant assumed legal and equitable duties and knew, or should have known, that it was responsible for protecting Plaintiff's and Class members' PII from unauthorized disclosure.

Defendant Knew That Criminals Target PII

42. At all relevant times, Defendant knew or should have known that Plaintiff's and all other Class members' PII was a target for malicious actors. Despite such knowledge, Defendant failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class members' PII from cyber-attacks that Defendant should have anticipated and guarded against.

[21] *Id.* at 1.

43. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches preceding the date of the Data Breach, which has been widely reported in the last few years.

44. In the wake of the significant rise in data breaches, the Federal Trade Commission has also issued an abundance of guidance for companies and institutions that maintain individuals' PII.[22]

45. Due to the notoriety of cyberattacks on systems like Defendant's, several other government entities have also issued warnings to potential targets so that they may be alerted and prepared for a potential attack like the Data Breach.

46. In light of the high-profile data breaches and a wealth of relevant guidance and news reports at Defendant's disposal, Defendant knew or should have known that cybercriminals would target its electronic records and employees' PII.

47. These data breaches have been a consistent problem for the past several years, providing Defendant sufficient time and notice to improve the security of their systems and engage in stronger, more comprehensive cybersecurity practices.

48. PII is a valuable property right.[23] The value of PII as a commodity is measurable.[24] "Firms are now able to attain significant market valuations by employing business models

---

[22] *See, e.g., Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N., https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last visited Apr. 5, 2024).

[23] *See* Marc van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFO. AND COMMC'N. TECH. 26 (May 2015), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible . . . .").

[24] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black*

predicated on the successful use of personal data within the existing legal and regulatory frameworks."[25] American companies are estimated to have spent over $19 billion in 2019 on acquiring consumers' personal data.[26] In fact, it is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

49. Because of its real value and the recent large-scale data breaches, identity thieves and cybercriminals have openly posted credit card numbers, Social Security numbers, and other PII directly on various Internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

50. Consumers place a high value on the privacy of their PII. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[27]

Market, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192.

[25] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD 4 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[26] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERT. BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

[27] Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, 22(2) INFO. SYS. RSCH. 254 (June 2011), https://www.jstor.org/stable/23015560?seq=1.

51. Given these factors, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

52. Therefore, Defendant clearly knew or should have known of the risks of data breaches and thus should have ensured that adequate protections were in place, particularly given the nature of the PII stored in its unprotected files and the massive amount of PII it maintains.

Theft of PII has Grave and Lasting Consequences for Victims.

53. Data breaches are more than just technical violations of their victims' rights. By accessing a victim's personal information, the cybercriminal can ransack the victim's life: withdraw funds from bank accounts, get new credit cards or loans in the victim's name, lock the victim out of their financial or social media accounts, send out fraudulent communications masquerading as the victim, file false tax returns, destroy their credit rating, and more.[28]

54. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[29] In addition, identity thieves may obtain a job using the victim's Social Security Number, rent a house, or receive medical

[28] *See* Laura Pennington, *Recent Data Breach Trends Mean Your Info Was Likely Stolen Last Year*, TOP CLASS ACTIONS (Jan. 28, 2019), https://topclassactions.com/lawsuit-settlements/privacy/data-breach/875438-recent-data-breach/.

[29] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official state or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

services in the victim's name, and they may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[30]

55. Indeed, Attorney Steven Weisman, the editor of Scamicide.com, says that hackers can easily use the last four digits of people's Social Security numbers, as was exposed in the Data Breach, to determine the first five digits themselves, since "they relate to where you live and where your card was issued."[31]

56. Identity theft victims are frequently required to spend many hours and large sums of money repairing the adverse impact on their credit.

57. Indeed, Plaintiff has already begun the long and arduous process of preventing further harm and injury resulting from the Data Breach. After the Data Breach, an unauthorized actor hacked and emptied Plaintiff's bank account, and Plaintiff spent time closing that account and opening a new one. Plaintiff has also suffered emotional distress as a result of the Data Breach and subsequent injuries.

58. As the United States Government Accountability Office noted in a June 2007 report on data breaches ("GAO Report"), identity thieves use identifying data such as Social Security Numbers to open financial accounts, receive government benefits, and incur charges and credit in a person's name.[32] As the GAO Report states, this type of identity theft is more harmful than any

---

[30] *See Warning Signs of Identity Theft*, FED. TRADE COMM'N, https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft (last visited Apr. 5, 2024).

[31] Alanna Flood & Amy Phillips, *Social Security numbers of some Xfinity customers vulnerable in latest data breach: What to know*, THE HILL (Dec. 30, 2023), https://thehill.com/homenews/4381585-social-security-numbers-of-some-xfinity-customers-vulnerable-in-latest-data-breach-what-to-know/.

[32] *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, U.S. GOV'T ACCOUNTABILITY OFF. (June 2007), https://www.gao.gov/new.items/d07737.pdf.

other because it often takes time for the victim to become aware of the theft, and the theft can adversely impact the victim's credit rating.

59. In addition, the GAO Report states that victims of this type of identity theft will face "substantial costs and inconveniences repairing damage to their credit records" and their "good name."[33]

60. There may be a time lag between when PII is stolen and when it is used.[34] According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[35]

61. Such personal information is such a crucial commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cybercriminals have openly posted stolen credit card numbers, Social Security Numbers, and other PII directly on various Internet websites, making the information publicly available.

62. Due to the highly sensitive nature of Social Security numbers, theft of Social Security numbers in combination with other PII (e.g., name, address, date of birth) is akin to having

---

[33] *Id.* at 2, 9.

[34] For example, on average, it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information. John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9, 12 (2019), https://www.iiisci.org/Journal/PDV/sci/pdfs/IP069LL19.pdf.

[35] U.S. GOV'T ACCOUNTABILITY OFF., *supra* n. 32 at 29 (emphasis added).

a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who companies employ to find flaws in their computer systems, stating, "If I have your name and your Social Security number and you haven't gotten a credit freeze yet, you're easy pickings."[36]

63. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft, and some need over a year.[37]

64. Plaintiff and Class members must vigilantly monitor their financial accounts and the accounts of their family members for many years to come.

65. It is within this context that Plaintiff and all other Class members must now live with the knowledge that their PII is forever in cyberspace and was taken by people willing to use that information for any number of improper purposes and scams, including making the information available for sale on the black-market.

Damages Sustained by Plaintiff and the Other Class Members

66. Plaintiff and all other Class members have suffered injury and damages, including, but not limited to (i) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) deprivation of the value of their PII, for which there is a well-established national and international market; (iv) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft and medical

---

[36] Patrick Lucas Austin, *'It is Absurd.' Data Breaches Show It's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019, 3:39 P.M.), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

[37] *2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, Their Families, Friends and Workplaces*, IDENTITY THEFT RES. CTR., https://www.idthecenter.org/identity-theft-aftermath-study/ (last visited Apr. 5, 2024).

identity theft they face and will continue to face; and (v) overpayment for the services that were received without adequate data security.

CLASS ALLEGATIONS

67. This action is brought and may be properly maintained as a class action pursuant to Rule 23(b)(2) and (3) of the Federal Rules of Civil Procedure.

68. Plaintiff brings this action on behalf of himself and all members of the following Class of similarly situated persons:

> All persons whose PII was accessed in the Data Breach by unauthorized persons, including all persons who were sent a notice of the Data Breach.

69. Plaintiff reserves the right to amend the above definition or to propose other or additional classes in subsequent pleadings and/or motions for class certification.

70. Plaintiff is a member of the Class.

71. Excluded from the Class are Bartlett Dairy, Inc. and its affiliates, parents, subsidiaries, officers, agents, and directors, the judge(s) presiding over this matter, and the clerks of said judge(s).

72. This action seeks both injunctive relief and damages.

73. Plaintiff and the Class satisfy the requirements for class certification for the following reasons:

74. **Numerosity of the Class.** The members in the Class are so numerous that joinder of all Class members in a single proceeding would be impracticable. While the exact number of Class members is unknown at this time, Class members are readily identifiable in Defendant's records, which will be a subject of discovery. Upon information and belief, there are millions of Class members in the Class.

75. **Common Questions of Law and Fact.** There are questions of law and fact common to the Class that predominate over any questions affecting only individual members, including:

a. Whether Defendant's data security systems prior to the Data Breach met the requirements of relevant laws;
b. Whether Defendant's data security systems prior to the Data Breach met industry standards;
c. Whether Defendant owed a duty to Plaintiff and Class members to safeguard their PII;
d. Whether Defendant breached its duty to Plaintiff and Class members to safeguard their PII;
e. Whether Defendant failed to provide timely and adequate notice of the Data Breach to Plaintiff and Class members;
f. Whether Plaintiff's and Class members' PII was compromised in the Data Breach;
g. Whether Plaintiff and Class members are entitled to injunctive relief; and
h. Whether Plaintiff and Class members are entitled to damages as a result of Defendant's conduct.

76. **Typicality.** The claims or defenses of Plaintiff are typical of the claims or defenses of the proposed Class because Plaintiff's claims are based upon the same legal theories and same violations of law. Plaintiff and Class members all had their PII stolen in the Data Breach. Plaintiff's grievances, like the proposed Class members' grievances, all arise out of the same business practices and course of conduct by Bartlett.

77. **Adequacy of Representation.** Plaintiff will fairly and adequately represent the Class on whose behalf this action is prosecuted. Their interests do not conflict with the interests of the Class.

78. Plaintiff and their chosen attorneys -- Finkelstein, Blankinship, Frei-Pearson & Garber, LLP ("FBFG") -- are familiar with the subject matter of the lawsuit and have full knowledge of the allegations contained in this Complaint. In particular, FBFG has been appointed as lead counsel in several complex class actions across the country and has secured numerous favorable judgments in favor of its clients, including in cases involving data breaches. Plaintiff's

Counsel are competent in the relevant areas of the law and have sufficient experience to vigorously represent the Class members. Finally, Plaintiff's Counsel possess the financial resources necessary to ensure that the litigation will not be hampered by a lack of financial capacity and is willing to absorb the costs of the litigation.

79. **Predominance.** The common issues identified above arising from Defendant's conduct predominate over any issues affecting only individual Class members. The common issues hinge on Defendant's common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff on behalf of themselves and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

80. **Superiority.** A class action is superior to any other available method for adjudicating this controversy. The proposed class action is the surest way to fairly and expeditiously compensate such a large number of injured persons, to keep the courts from becoming paralyzed by hundreds -- if not thousands -- of repetitive cases, and to reduce transaction costs so that the injured Class members can obtain the most compensation possible.

81. Class treatment presents a superior mechanism for fairly resolving similar issues and claims without repetitious and wasteful litigation for many reasons, including the following:

a. It would be a substantial hardship for most individual members of the Class if they were forced to prosecute individual actions. Many members of the Class are not in the position to incur the expense and hardship of retaining their own counsel to prosecute individual actions, which, in any event, might cause inconsistent results.

b. When the liability of Defendant has been adjudicated, the Court will be able to determine the claims of all members of the Class. This will promote global relief and judicial efficiency in that the liability of Defendant to all Class members, in terms of monetary damages due and terms of equitable relief, can be determined in this single proceeding rather than in multiple individual proceedings where there will be a risk of inconsistent and varying results.

c. A class action will permit an orderly and expeditious administration of the Class claims, foster economies of time, effort, and expense, and ensure uniformity of

decisions. If Class members are forced to bring individual suits, the transactional costs, including those incurred by Defendant, will increase dramatically, and the courts will be clogged with a multiplicity of lawsuits concerning the very same subject matter, with identical fact patterns and the same legal issues. A class action will promote a global resolution and uniformity of relief to the Class members and Defendant.

d. This lawsuit presents no difficulties that would impede its management by the Court as a class action. The class certification issues can be easily determined because the Class includes only current or former employees of Defendant, the legal and factual issues are narrow and easily defined, and the Class membership is limited. The Class does not contain so many persons that would make the Class notice procedures unworkable or overly expensive. The identity of the Class members can be identified from Defendant's records, such that direct notice to the Class members would be appropriate.

82. **Injunctive relief.** Defendant has acted or refused to act on grounds generally applicable to the Class as a whole, thereby making appropriate final injunctive or equitable relief on a class-wide basis.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

83. Plaintiff and Class members reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

84. As a condition of entering into employment contracts with Defendant, Plaintiff and Class members were required to and did provide Defendant with their PII.

85. By collecting and storing their PII and using it for commercial gain, at all times relevant, Defendant owed a duty to Plaintiff and all other Class members to exercise reasonable care in safeguarding and protecting their PII in its possession, custody, or control.

86. Defendant owed a duty of care to Plaintiff and Class members to provide data security consistent with statutory and industry standards and to ensure that their systems and networks and the personnel responsible for them adequately protected the PII.

87. Defendant knew the risks of collecting and storing Plaintiff's and all other Class members' PII and the importance of maintaining secure systems. Defendant knew of the many data breaches that targeted companies that store PII in recent years.

88. Given the sensitivity and value of the PII of its employees that Defendant maintains and the resources at its disposal, Defendant should have identified the vulnerabilities in their systems and prevented the Data Breach from occurring.

89. Defendant breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII entrusted to them -- including Plaintiff's and Class members' PII.

90. Plaintiff and Class members are a well-defined, foreseeable, and probable group of current and former employees that Defendant was aware, or should have been aware, could be injured by inadequate data security measures.

91. Plaintiff and Class members have no ability to protect their PII that was or remains in Defendant's possession.

92. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII to unauthorized individuals.

93. But for Defendant's negligent conduct and breach of the above-described duties owed to Plaintiff and Class members, their PII would not have been compromised.

94. Defendant's conduct was grossly negligent and departed from reasonable standards of care, including but not limited to failing to adequately protect Plaintiff's and Class members' PII and failing to provide them with timely notice that their PII had been compromised.

95. Neither Plaintiff nor Class members contributed to the Data Breach and subsequent misuse of their PII as described in this Complaint.

96. By failing to provide timely and complete notification of the Data Breach to Plaintiff and Class members, Defendant prevented them from proactively securing their PII and mitigating the associated threats.

97. As a result of Defendant's above-described wrongful actions, inaction, and lack of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other Class members have suffered and will continue to suffer economic damages and other injury and actual harm in the form of, inter alia: (i) a substantially increased risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

COUNT II
NEGLIGENCE PER SE

98. Plaintiff and Class members reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

99. Defendant had duties by statute to ensure that all information it collected and stored was secure and that it maintained adequate and commercially reasonable data security practices to ensure the protection of Plaintiff's and Class members' PII.

100. Defendant's duties arise from, *inter alia*, Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as Defendant, of failing to employ reasonable measures to protect and secure PII.

101. The FTC has published numerous guides for businesses that highlight the importance of implementing reasonable data security practices. In 2016, the FTC updated its publication establishing cybersecurity guidelines for businesses, which makes thorough recommendations, including, but not limited to, for businesses to protect the personal customer information they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[38]

102. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTCA. Orders resulting from these actions further clarify the measures businesses such as Defendant must take to meet their data security obligations and effectively put Defendant on notice of these standards.

[38] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N. (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

103. Defendant violated Section 5 of the FTCA and similar state statutes by failing to use reasonable measures to protect Plaintiff's and all Class members' PII and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtains and stores and the foreseeable consequences of a data breach involving PII, including, specifically, the substantial damages that would result to Plaintiff and other Class members.

104. Defendant's violation of these federal and state laws constitutes negligence per se.

105. Plaintiff and Class members are within the class of persons that Section 5 of the FTCA was intended to protect.

106. The harm occurring as a result of the Data Breach is the type of harm against which Section 5 of the FTCA was intended to guard.

107. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class members' PII to unauthorized individuals.

108. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of Defendant's violation of Section 5 of the FTCA. Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia: (i) a substantially increased risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their

PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

109. Defendant's violation of the FTCA and state statutes constitutes negligence *per se* for purposes of establishing the duty and breach elements of Plaintiff's negligence claim. Those statutes were designed to protect a group to which Plaintiff belongs and to prevent the type of harm that resulted from the Data Breach.

110. Defendant owed a duty of care to the Plaintiff and the members of the Class because they were foreseeable and probable victims of any inadequate security practices.

111. It was foreseeable that Defendant's failure to use reasonable measures to protect PII and to provide timely notice of the Data Breach would result in injury to Plaintiff and other Class members. Further, the breach of security, unauthorized access, and resulting injury to Plaintiff and the members of the Class were reasonably foreseeable.

112. It was therefore foreseeable that the failure to adequately safeguard PII would result in one or more of the following injuries to Plaintiff and the members of the proposed Class: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

COUNT III
BREACH OF FIDUCIARY DUTY

113. Plaintiff and Class members reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

114. Plaintiff and Class members gave Defendant their PII in confidence, believing that Defendant would protect that information. Plaintiff and Class members would not have provided Defendant with this information had they known it would not be adequately protected. Defendant's acceptance and storage of Plaintiff's and Class members' PII created a fiduciary relationship between Defendant and Plaintiff and Class members.

115. In light of this relationship, Defendant has a fiduciary duty to act primarily for the benefit of Plaintiff and Class members upon matters within the scope of their relationship, which includes safeguarding and protecting Plaintiff's and Class members' PII.

116. Defendant breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and Class members' PII and otherwise failing to safeguard Plaintiff's and Class members' PII that they collected.

117. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer injury, including, but not limited to (i) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) the improper compromise, publication, and theft of their PII; (iii) deprivation of the value of their PII, for which there is a well-established national and international market; (iv) lost time and money incurred, and future costs required, to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; (v) the continued risk to their

PII which remains in Defendant's possession; and (vi) overpayment for the services that were received without adequate data security.

COUNT IV
BREACH OF IMPLIED CONTRACT

118. Plaintiff and Class members reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

119. In connection with receiving employment, Plaintiff and all other Class members entered into implied contracts with Defendant.

120. When Plaintiff and Class members provided their PII to Defendant directly or indirectly as a pre-condition and in exchange for employment, they entered into implied contracts with Defendant.

121. Pursuant to these implied contracts, in exchange for the consideration and PII provided by Plaintiff and Class members, Defendant agreed to, among other things, and Plaintiff understood that Defendant would: (1) provide employment to Plaintiff and Class members; (2) implement reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII; and (3) protect Plaintiff's and Class members' PII in compliance with federal and state laws and regulations and industry standards.

122. The protection of PII was a material term of the implied contracts between Plaintiff and Class members, on the one hand, and Defendant, on the other.

123. Plaintiff and Class members performed their obligations under the implied contract when they provided Defendant with their PII and paid for the services from Defendant.

124. Plaintiff and Class members would not have entrusted their PII to Defendant in the absence of such an implied contract.

125. Had Plaintiff and Class members known that Defendant would not adequately protect its employees' and former employees' PII, they would not have agreed to employment by Defendant.

126. Defendant breached its obligations under its implied contracts with Plaintiff and Class members by failing to implement and maintain reasonable security measures to protect and secure their PII and security protocols and procedures to protect Plaintiff's and Class members' PII in a manner that complies with applicable laws, regulations, and industry standards.

127. Defendant's breach of its obligations under its implied contracts with Plaintiff and Class members directly resulted in the Data Breach and the injuries that Plaintiff and all other Class members have suffered from the Data Breach.

128. Plaintiff and all other Class members were suffered by Defendant's breach of implied contracts because (i) they contracted for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII has been breached; (v) they were deprived of the value of their PII, for which there is a well-established national and international market; (vi) lost time and money incurred, and future costs required, to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vii) overpayment for the services that were received without adequate data security.

COUNT V
UNJUST ENRICHMENT

129. Plaintiff and Class members reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

130. This claim is pleaded in the alternative to the breach of implied contract claim.

131. Plaintiff and Class members conferred a monetary benefit upon Defendant in the forms of (1) their provision of work and labor hours as employees and (2) the provision of their valuable PII. Indeed, upon acquiring the PII, Defendant was then able to utilize Plaintiff and class members as employees to help facilitate its business. The PII was thus used to generate additional revenue for Defendant.

132. Defendant accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class members. Defendant profited from these transactions and used the PII of Plaintiff and Class members for business purposes.

133. Upon information and belief, Defendant, like most other corporate entities, funds their data security measures entirely from their general revenue, which includes money paid by Plaintiff and Class members.

134. As such, a portion of the payments made by or on behalf of Plaintiff and Class members is or should have been used to provide a reasonable level of data security.

135. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure its employees' PII.

136. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant calculated that it would avoid its data security obligations at the expense of Plaintiff and Class members by utilizing less expensive and less effective security measures.

137. As a direct and proximate result of Defendant's failure to provide the requisite security, Plaintiff and Class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and

procedures that Plaintiff and Class members contracted for and those payments without reasonable data privacy and security practices and procedures that they received.

138. Defendant should not be permitted to retain the money belonging to Plaintiff and Class members because Defendant failed to adequately implement the data privacy and security procedures for itself that Plaintiff and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

139. Defendant should be compelled to provide all unlawful proceeds received by it as a result of its conduct and the resulting Data Breach alleged herein for the benefit of Plaintiff and Class members.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the Class, respectfully request that the Court enter judgment in his favor and against Defendant as follows:

A. Certifying that Class as requested herein, appointing the named Plaintiff as Class representative and the undersigned counsel as Class Counsel;

B. Requiring that Defendant pays for notifying the members of the Class of the pendency of this suit;

C. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

D. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of himself and the Class, seeks appropriate injunctive relief designed to prevent Defendant from experiencing another data breach by adopting and implementing best data security practices to safeguard PII and to provide or extend additional

credit monitoring services and similar services to protect against all types of identity theft and medical identity theft.

E. Awarding Plaintiff and the Class prejudgment and post-judgment interest to the maximum extent allowable;

F. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable, together with their costs and disbursements of this action; and

G. Awarding Plaintiff and the Class such other and further relief as the Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: April 11, 2024

Respectfully submitted,

/s/ Todd S. Garber
Todd S. Garber
Andrew C. White
FINKELSTEIN, BLANKINSHIP FREI-PEARSON & GARBER, LLP
One North Broadway, Suite 900
White Plains, New York 10601
Tel.: (914) 298-3281
tgarber@fbfglaw.com
awhite@fbfglaw.com

Attorneys for Plaintiff and the Proposed Class